DEPARTMENT OF TRANSPORTATION
SHORT GUIDE TO HANDLING SENSITIVE SECURITY INFORMATION (SSI) FOR EXTERNAL PARTIES

1) **Do not leave SSI unattended** on your desk, in your office or any other place you carry it. Remember to check for SSI, when you leave for meetings, lunch, brief trips to the restroom, filing room, a colleague's office or before you leave at night. In these cases be sure to place it in a locked desk drawer, or locked file cabinet.

2) **Turn off or lock your computer when working with SSI** before you leave your desk to ensure that no SSI is compromised.

3) **Only share SSI documents or information with a covered party who has a need to know**. When in doubt, contact the DOT Office of Intelligence, Security, and Emergency Response at (202) 366-6525 or SSI@dot.gov. Do not discuss SSI at all with friends or family (unless they are covered parties with a need to know), and do not discuss SSI with colleagues in public places**. If you need to discuss SSI over the telephone, make every effort to use a land line** and be aware of your surroundings. If forced to discuss SSI in a public place, use common sense and discuss as privately as possible - not within the ear-shot of other people. If it is necessary to mention SSI over a cellular phone, take all precautions to discuss sparingly and privately.

4) Do not deliver any SSI to anyone by leaving it unattended on their desk; **personally hand deliver any SSI** to the intended recipient. You have a duty to make sure that the SSI recipient knows that the document(s) contain SSI so they can take appropriate steps concerning SSI handling protection.

5) When carrying or delivering SSI**, place in an unmarked folder or envelope**.

6) **Do not take SSI home**, either hard or soft-copy, without written permission from your supervisor. If you do take SSI home, always keep the SSI on your person (ideally in a locked briefcase) during transit and protect as you would in your office.

7) **Password-protect** all SSI documents sent via e-mail. **Do not include the password in the body and/or e-mail introduction forward.** Passwords shall conform to the following guidelines: eight character minimum length; at least one letter capitalized, contain at least one number; and not be a word in the dictionary. Take the correct password precaution and disclose the password to the recipient in person or by phone.

8) **SSI should always be marked** as such with a protective marking in the header and a distribution limitation statement in the footer (see below). For paper records, the protective marking must be at the top and the distribution limitation statement at the bottom of (1) the outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover; (2) any title page; and (3) each page of the document. *When in doubt whether a document should be marked SSI, contact the DOT Office of Intelligence, Security, and Emergency Response at (202) 366-6525 or SSI@dot.gov.*

9) **No SSI should be posted or appear on your Internet or Intranet web sites without prior approval**. It is your duty to be diligent in observing any SSI that erroneously appears and contact the appropriate parties to have it removed. You may contact the DOT Office of Intelligence, Security, and Emergency Response at (202) 366-6525 or SSI@dot.gov for assistance.

10) **Properly dispose of all SSI in your possession that you no longer need** (e.g., extra copies, obsolete versions, etc.) by using a shredder or cutting manually to less than ½ inch. SSI on electronic media should be destroyed so as to render the media unusable and preclude its reconstruction.

Protective Marking (header): SENSITIVE SECURITY INFORMATION

Distribution Limitation (footer):

WARNING: **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a ''need to know'', as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of**